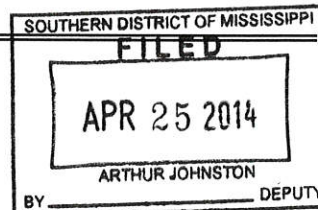


UNITED STATES DISTRICT COURT

for the

Southern District of Mississippi



United States of America)

v.)

OLUTOYIN OGUNLADE)

Case No. 1:14mj 31

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of September 2012 in the county of Harrison in the
Southern District of Mississippi and elsewhr, the defendant(s) violated:

Code Section

18 United States Code 1349

Offense Description

Attempt and conspiracy to commit fraud

This criminal complaint is based on these facts:

See attached affidavit incorporated herein.

☒ Continued on the attached sheet.

Complainant's signature

Brent Druery, S/A HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: 04/25/2014

Judge's signature
City and state: Gulfport, Mississippi

John M. Roper, Chief U.S. Magistrate

Printed name and title

AFFIDAVIT

I, Brent Druery, a duly sworn Special Agent with Homeland Security Investigations (HSI), within U.S. Immigration and Customs Enforcement (ICE), do hereby depose and state:

1. I am assigned to the HSI Gulfport, Mississippi, office. I have been trained specifically in the investigation and elements of federal crimes at the Federal Law Enforcement Training Center at Glynco, Georgia. I have approximately twelve (12) years of experience as a federal law enforcement officer and criminal investigator.

2. I am statutorily empowered to investigate violations of Title 18 of the United States Code and other federal statutes.

3. The information contained in this affidavit has been gathered from various law enforcement officers within Homeland Security Investigations

4. Since October of 2011, Homeland Security Investigations has investigated a West African transnational organized crime enterprise (TOC) involved in numerous complex financial fraud schemes via the internet. The West African TOC, identified as the Yahoo Boys Criminal Organization, perpetrates the schemes involving a complex web of mass marketing fraud perpetuating the criminal underground economy via the illegal sales of personal identifying information and compromised credit card/banking information on the internet. The mass marketing fraud includes romance scams, re-shipping scams, fraudulent check scams, work-at-home scams, along with bank, financial and credit card account take-overs. Members of the Yahoo Boys Criminal Organization have historically utilized numerous email accounts to facilitate their online financial fraud schemes. Analysis has revealed identified and unidentified co-conspirator email

accounts assisting in the laundering of financial fraud proceeds. This complaint involves an individual who is participating in the fraud schemes and the laundering of the proceeds with individuals indicted in the Southern District of Mississippi, in Cause No.

1:14cr33HSO-JMR.

5. During the course of the investigation, email accounts PETERLAWSON5050@YAHOO.COM and REDARMY_TX_HOST@YAHOO.COM have been identified as being utilized by the Yahoo Boy Criminal Organization. Analysis of the accounts has revealed that both accounts have been actively used by known co-conspirators located in Canada and Nigeria in furtherance of numerous different financial fraud schemes, including account take-overs. Analysis has further revealed that the two identified targets routinely conspire with additional members of the Yahoo boy Criminal Organization located within the United States to launder the illegally gained financial fraud proceeds. The below listed scheme is included in Cause No. 1:14cr33HSO-JMR, and exemplifies the transnational conspiracy and identifies a significant member of the organization located in Brooklyn, New York, tasked with laundering account takeover proceeds.

6. Analysis of target email account

REDARMY_TX_HOST@YAHOO.COM revealed on September 01, 2013, at approximately 1932 hours, REDARMY_TX_HOST@YAHOO.COM sent an email to PETERLAWSON5050@YAHOO.COM, with the subject line "200." Attached to the email were approximately 200 AOL screen names and passwords along with the owner's personal identifying information and banking/credit card data. Within the attachment was complete information personal identifying information (PII), passwords, mother's

maiden name, driver license, banking and credit card information with PIN number for victim G.A.

7. On October 03, 2013, at approximately 1210 hours, NEIL50070@YAHOO.CA sent an email to PETERLAWSON5050@YAHOO.COM, with the subject line "KANGA MEJI." The narrative portion of the email contained the below Wells Fargo bank account number utilized on October 21, 2013, to request the ACH transfer of \$34,950.00, from the victim's account:

"1.SCOTT F INMAN ACC# 5791119968
ROUT# 026012881 TOLL FREE# 1800-869-3557
USER/ inman69 PASSW/scobo57 PIN/ 3111"

8. On October 14, 2013, at approximately 1849 hours, PETERLAWSON5050@YAHOO.COM sent an email to himself with the subject line "wells fago paper." The narrative portion of the email contained:

"G. A.
659 S. BOARDWAY STREET BOOTH M1
LOS ANGELES, CA 90014
ACCOUNT# 5791119968
ROUTING# 026012881
BRANCH ADDRESS"

9. Customers G.A. and A.A., holders of a TD Ameritrade account were victims of identity theft and account takeover fraud. TD Ameritrade records revealed the following unauthorized activity conducted on the account:

10. From October 14, 2013, to November 01, 2013, TD Ameritrade received numerous calls from a male caller impersonating victim G.A. Thirty-three (33) of the calls were from phone number 647-705-6938, previously identified within email account peterlawson5050@yahoo.com. On October 14, 2012, TD Ameritrade received a request for an Automated Clearing House (ACH) Bank Set-Up form to be emailed to

GUUYZAK@AOL.COM. On October 17, 2013, TD Ameritrade received ACH Bank Set-Up form and a voided check to add bank instructions for a Wells Fargo account located in Chicago, IL, allegedly in the name of victim G.A. The form and check were faxed from 905-232-9320.

11. On October 21, 2013, TD Ameritrade received an ACH request for \$34,950.00 to be transferred to the aforementioned Wells Fargo bank account.

12. On October 28, 2013, at approximately 1100 hours, PETERLAWSON5050@YAHOO.COM sent an email to HALLMARKREG@GMAIL.COM, with the subject line "frm filla...., na paper I want pls sir....." The narrative portion of the email stated:

CITI BANK PAPER
G. A. & A. A.
659 S.BROADWAY STREET BOOTH M1
LOS ANGELES, CA 90014

ACCOUNT # 4981987065
ROUTING # 021000089

BANK ADDRESS
1 PENNS WAY
NEW CASTLE
DE - 19720

13. On October 28, 2013, an order to sell 2,000 shares of Oracle (ORCL) from The TD Ameritrade account of victim G.A. was placed. On October 29, 2013 TD Ameritrade received an ACH Bank Set-Up form and voided check to add bank instructions for Citibank located in New Castle, DE allegedly in the names of victims G.A. and A.A. The form and check were again faxed from 905-232-9320. On November 01, 2013, TD Ameritrade received an ACH transfer for \$33,480.00 to the aforementioned

Citibank account. Subsequent investigation revealed the owners of the TD Ameritrade account had not made or authorized the transfer requests and were the victims of fraud.

14. Comparison of IP addresses captured by TD Ameritrade and the IP addresses for email account PETERLAWSON5050@YAHOO.COM, proved identical matches on many of the dates and times the victims' account was accessed.

15. On November 20, 2013, victims G.A. and A.A. signed an affidavit and provided a Los Angeles Police Department Police Report regarding the identity theft and account takeover fraud to TD Ameritrade.

16. Wells Fargo banking records for the account that originally received the \$34,950.00 of financial fraud proceeds revealed that from October 22, 2013, to November 1, 2013, eight purchases totaling \$5,497.76 occurred at Rite Aid stores from the Wells Fargo account. Records from Rite Aid revealed that the identified purchases were for Green Dot MoneyPaks. Green Dot fraud department revealed that the identified MoneyPak funds were utilized to load the below listed pre-paid cards:

Card Number	Card Name	Card Holder Address
4984040003300447	Oluyitan Olagoke	921 E 85th St Brooklyn, NY
4692080017371987	Clarence Lebus	1019 Rogers Ave Brooklyn, NY
4692080016913391	Lance Leu	1019 Rogers Ave Brooklyn, NY
4418580222404435	Bradly Abrams	950 Rutland Rd Apt 204 Brooklyn, NY

17. Records from Green Dot revealed that pre-paid card 4984040003300447 in the name of Oluyitan Olagoke had several withdrawals at ATM machines operated by JPMorgan Chase. Records from Bancorp Bank revealed that pre-paid card 4692080017371987 in the name of Clarence Lebus also had withdrawals at ATM machines operated by JPMorgan Chase bank.

18. A photo request to JPMorgan Chase revealed surveillance photographs for

transactions at the following branches and times:

Oluyitan Olagoke (4984040003300447)

Date	Time	Bank Location	Amount
11/6/2013	11:40PM	391 Eastern Pkwy Brooklyn, NY	\$ 403.00
12/24/2013	3:08PM	1599 Flatbush Ave Brooklyn, NY	\$ 403.00
1/18/2014	6:29AM	1128 Eastern Pkwy Brooklyn, NY	\$ 403.00

Clarence Lebus (4692080017371987)

Date	Time	Bank Location	Amount
12/24/2013	3:08PM	1599 Flatbush Ave Brooklyn, NY	\$ 483.00
1/18/2014	9:55PM	402 Myrtle Ave Brooklyn, NY	\$ 483.00
1/21/2014	12:27PM	1599 Flatbush Ave Brooklyn, NY	\$ 483.00
1/22/2014	12:53PM	9601 Foster Ave Brooklyn, NY	\$ 483.00
1/23/2014	8:48AM	1764 Rockaway Pkwy Brooklyn, NY	
1/23/2014	1:46PM	1599 Flatbush Ave Brooklyn, NY	\$ 403.00
1/26/2014	5:33PM	615 Eighth Ave Brooklyn, NY	\$ 483.00
1/27/2014	9:40PM	9601 Foster Ave Brooklyn, NY	\$ 483.00

19. Analysis of the photographs received from JPMorgan Chase, related to the ATM transactions conducted utilizing pre-paid visa cards 4984040003300447 and 4692080017371987, revealed both accounts were being controlled by the same subject. Specifically, both accounts were utilized at the same ATM at the same exact time on December 24, 2013. Further analysis of the photographs revealed the subject utilizing the accounts was a heavy-set, bald, black male. The photographs revealed the subject consistently wore a winter hat lined with grey fur, a long sleeve shirt with a reverse American flag on the right shoulder, and a sleeveless winter vest.

20. Records from Wells Fargo bank regarding account number 5791119968 further revealed that from October 23, 2013, to November 3, 2013, eight additional purchases totaling \$5,968 occurred at Wal-Mart stores. Records from Wal-Mart show that the identified purchases were for eight MoneyGram money orders. MoneyGram records

revealed that two of the eight MoneyGram money orders were purchased on October 26, 2013, and October 31, 2013, at Wal-Mart store #5293 located at 77 Green Acres Rd, Valley Stream, NY, totaling \$1,392. Both money orders were paid to the order of a Jerry Camera with a listed address in Cleveland, OH 44128.

21. Records from MoneyGram further revealed that MoneyGram money orders 20528042791 and 20528042869 were deposited into a Huntington Bank account in the name of Jerry Camera on November 20, 2013. Huntington Bank records for the account revealed purchases at Wal-Mart store #5293 located at 77 Green Acres Rd, Valley Stream, NY on December 20, 2013, and January 30, 2014, totaling \$4,564.20. A review of Wal-Mart records reflect these purchases were for six MoneyGram money orders totaling \$4,560. Of the six money orders purchased, four were paid to the order of Lee Hieronymus with an account at Bank of America. A review of the MoneyGram money orders revealed that three of the money orders paid to Lee Hieronymus were deposited at a Bank of America Branch at 1580 Flatbush Ave., Brooklyn NY on or around 12:18pm on December 26, 2013. The total value of the three money orders deposited was \$2,060. On or around 11:01 am on February 3, 2014, the fourth money order totaling \$950 paid to the order of Lee Hieronymus was deposited at a Bank of America branch on 1502 Kings Highway, Brooklyn, NY.

22. Photos obtained from Bank of America for the two identified transactions reveal the same black male depositing the money orders into the Lee Hieronymus Bank of America account. A photo comparison of the of the black male depositing the money orders into the Lee Hieronymus account along with the photos of the black male


previously identified conducting the transactions at JPMorgan Chase ATMs provide a positive match.

23. Queries of the Treasury Enforcement Communications System (TECS) database for the address associated with the four identified pre-paid cards revealed numerous positive hits for address 950 Rutland Rd., Brooklyn, NY. Further investigation into the records associated with address 950 Rutland Rd., Brooklyn, NY, revealed subject OLUTOYIN O. OGUNLADE, date of birth 08/19/1973, as being associated with the address, and being the subject of a closed credit card fraud investigation. Further queries for subject OLUTOYIN O. OGUNLADE reveal an I-130, Petition for Alien Relative, which listed OGUNLADE's address as 921 East 85th Street Apt. 2, Brooklyn, NY. This address was a positive match for the address used for pre-paid card 4984040003300447 in the name of Oluyitan Olagoke.

24. Queries of the National Law Enforcement Telecommunications System (NLETS) database for subject OLUTOYIN OGUNLADE, date of birth 8/19/1973, reveal a current New York driver's license and listed address of 1018 E. 87th Street #03, Brooklyn, NY. A photo comparison of the driver's license photograph of OLUTOYIN OGUNLADE with the surveillance photographs of the black male conducting transactions associated with the Lee Hieronymus Bank of America account and the pre-paid visa cards 4984040003300447 (Oluyitan Olagoke) and 4692080017371987 (Clarence Lebus), provide an identical match, thus identifying OLUTOYIN OGUNLADE as the subject conducting the financial transactions.

25. Based on these underlying facts and circumstances, as set forth above, it is my

belief there is probable cause that OLUTOYIN OGUNLADE did: did knowingly and willfully conspire with others known and unknown to violate Section 1349, Title 18 United States code, attempt and conspiracy to commit bank fraud as prohibited by 18 United States Code § 1344 and wire fraud as prohibited by 18 United States Code § 1343.



Brent Druery
Special Agent
Homeland Security Investigations

Sworn and subscribed before me the 25th day of April, 2014.



JOHN M. ROPER
CHIEF UNITED STATES MAGISTRATE JUDGE